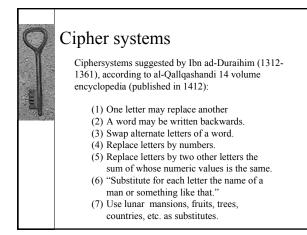
| 9 | Modern Beginnings       |  |
|---|-------------------------|--|
|   |                         | use of monoalphabetic ciphers for administrative use   |
|   | (In the name            | 900 AD Al-Kindī:<br>"A Manuscript on Deciphering<br>Cryptographic Messages"<br>(first systematic description of<br>using frequency analysis to<br>break a substitution cipher) |
|   | Taken from Simon Singh. | The Code Book.   |

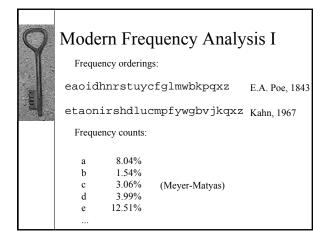


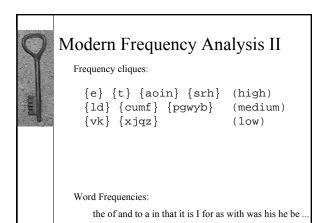
## Frequency Analysis

1412 AD Al-Qalqashandi: detailed description of frequency analysis in Arabic based on earlier writings by Ibn ad-Duraihim (1300 AD)

"When you want to solve a message which you have received in code, begin first of all by counting the letters, and then count how many times each symbol is repeated and set down the totals individually." ...

"When you see that one letter occurs in the message more often than the rest, then assume that it is alif; then assume that the next most frequent is lām."





## Modern Frequency Analysis III

Word frequencies:

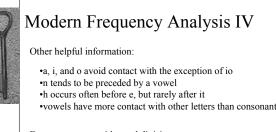
the of and to a in that it is I for as with was his he be .

Frequent bigrams:

th he an in er re on es ti at st en or nd to nt ed is ar

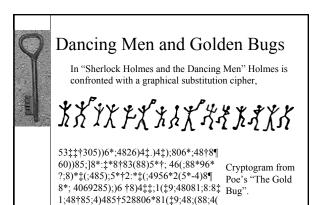
Frequent trigrams:

the ing and ion tio ent ere her ate ver ter tha ati for



For cryptograms with word divisions:

•t, o, s are frequent both as first and last letters
•a, i, h are frequent as first, but not last letters
•e, n, r are frequent as last, but not first letters



**‡**?3 4;48)4**‡**;161;:188;**‡**?;